A Mobile Edge Computing Enabled Spectrum Blockchain for the Internet of Spectrum Devices

1st Jian Yang[1], 2nd Guoru Ding[2], 3rd Xi Chen, 4th Linyuan Zhang,
5th Jiachen Sun, 6th Hangsheng Zhao
{yangjian_njust@foxmail.com[1], dr.guoru.ding@ieee.org[2],
chenxi@njust.edu.cn[3], zhanglinyuan5@163.com[4], sun_jiachen@outlook.com[5],
zhaohs@njupt.edu.cn[6]}*

The 63rd Institude, National Univ. of Defense Technology, Nanjing 210007, China[1],
College of Communication Engineering, Army Engineering Univ., Nanjing 210096, China[2],
School of Mechanical Engineering, Nanjing Univ. of Sci. & Tech., Nanjing 210094, China[3],
College of Communication Engineering, Army Engineering Univ., Nanjing 210096, China[4],
College of Communication Engineering, Army Engineering Univ., Nanjing 210096, China[5],
School of Telecommunications, Nanjing Univ. of Posts and Telecomm., Nanjing 210003, China[6]

Abstract. To achieve secure and immutable spectrum data monitoring and sharing, and further to realize accurate and reliable spectrum strategy customization, a mobile edge computing (MEC) enabled spectrum blockchain is developed for the internet of spectrum devices (IoSD). Specially, a three-stage consensus mechanism is designed to achieve secure and immutable spectrum data monitoring and sharing, and spectrum blockchain employs the edge-deployed personal wireless device to realize efficient storage of massive spectrum data and quickly response of spectrum strategy customization. The malicious behaviour of spectrum data falsification is employed as Byzantine attack to evaluate the security performance of the proposed MEC-enabled spectrum blockchain. Numerical simulations show the consensus mechanism identify the malicious behaviours with high probability of detection under a variety of scenarios.

Keywords: Spectrum blockchain, mobile edge computing, internet of spectrum device, consensus mechanism, Byzantine attack

1 Introduction

The flourishing of the mobile Internet and Internet of Things triggers the surgent traffic growth, and further aggravates the contradiction between the requirement of spectrum bandwidth and the limited spectrum supply. Spectrum sharing is widely recognized as an affordable, near-term method to ensure necessary network capacities [1]. Diversified spectrum sharing patterns (e.g. ISM bands and TV white spaces [2], cellular network and satellite system [3], LSA bands and unlicensed bands [4]) require full awareness of electromagnetic situation, including the current situation and future trends of electromagnetic environment, so as to

* This work is supported by the National Natural Science Foundation of China (Grant No. 61471395, No. 61301161, No. 61871398 and No. 61501510), Natural Science Foundation of Jiangsu Province (Grant No. BK20161125, No. BK20160034, and No. BK20150717), China Postdoctoral Science Foundation Funded Project (Grant No. 2018M633769). *(Corresponding authors: Hangsheng Zhao.)*

MOBIMEDIA 2019, June 29-30, Weihai, People's Republic of China

DOI 10.4108/eai.29-6-2019.2282647

achieve accurate and reliable customization of spectrum sharing strategies. Spectrum sharing strategy, known as the transmission information in time, frequency, spatial and energy domain [5], largely depends on the full knowledge of local electromagnetic environment, which further depends on spectrum sensing and spectrum-sensing-based spectrum inference. Therefore, how to obtain the massive spectrum data in an efficient and secure manner, becomes the key challenge in realizing accurate and reliable spectrum sharing.

Traditional, spectrum devices are grouped into two classes: spectrum monitoring devices (SMDs) and spectrum utilizing devices (SUDs). Nowadays, as more and more spectrum sensors are equipped on SUDs, SUDs gradually has considerable spectrum sensing capabilities, specifically for personal wireless devices (e.g. smartphones, tablets, and in-vehicle sensors). Consequently, employing personal wireless devices to collect spectrum data in crowd sensing manner is a promising solution. Then, lets introduce the emerging concept of the Internet of Spectrum Devices (IoSD) [6], which integrates the concepts of spectrum sharing, internet of things, and spectrum big data, and realizes by networking SMDs and SUDs to achieve efficient spectrum data sharing and exchanging.

However, on one hand, the various spectrum devices do not trust each other in IoSD, while some sensitive information, such as identities, locations, parameters, etc., are embedded in spectrum data [7]. The lack of privacy-preserving mechanism may prohibits the enthusiasm of data sharing. On the other hand, traditionally, SMDs devices are managed in a centralized mode and spectrum servers in charge of issuing spectrum sensing task and collecting spectrum data. Massive spectrum data are uploaded to the spectrum server and all SUDs download spectrum data from spectrum server [8]. As a result, storing enormous volume of spectrum data are not only costly to the spectrum servers, tremendous visit demands may also causes spectrum server downtime or unpredictable latency.

Thus, how to achieve secure and efficient spectrum data sharing between untrusted spectrum devices is essential in IoSD. As an emerging technology, blockchain is a public ledger that records transactions among untrusted users, secured by an appropriate consensus mechanism. The outstanding features of blockchain include immutability, irreversibility, decentralization, anonymity, and asymmetric encryption. Inspired by the concept of blockchain, the spectrum blockchain is designed to store spectrum data in secure, immutable, irreversible, and decentralized manner, with each spectrum block links to its predecessor via a cryptographic pointer. The anonymity and asymmetric encryption eliminate the risk of privacy leakage and guarantee the chronological appended spectrum blocks are immutability and irreversibility. Nevertheless, blockchain suffers from various disadvantages, particularly in terms of quickly consensus achievement in a large-scale network, energy consumption in consensus, and the storage requirements of the whole chain during the verification.

Recent years, a new trend in computing is happening with the function of clouds being increasingly moving towards the network edges [9]. Computing, network control, and storage are pushed to the network edge with the aim of reducing computing-latency and energy consumption. Considering SUDs generally apply *local* spectrum data to infer spectrum sharing strategy, it is unnecessary and costly to store massive spectrum data centrally in the spectrum server cloud. An accurate and reliable spectrum sharing are basically rely on efficient access of local spectrum data, i.e. spectrum data is considered to be generated and consumed in the same geographical area.

In this paper, we propose a mobile edge computing (MEC) enabled spectrum blockchain to address this issue. The main contributions of this paper are summarized as follows:

- We develop a MEC-enabled spectrum blockchain for IoSD. so as to achieve secure and immutable spectrum data monitoring and sharing in spectrum blockchain, with

the edge-deployed personal wireless devices are employed to realize efficient storage of massive spectrum data and quickly response of spectrum strategy customization.

- We design a three-stage consensus mechanism to defense the malicious behaviour of spectrum data falsification, which is a Practical Byzantine Fault Tolerance (PBFT) based Byzantine defense mechanism, and has the same function with the proof of work (PoW) in Bitcoin system.
- We evaluate security performance of the proposed MEC-enabled spectrum blockchain and our results show that the consensus mechanism of which identify the malicious behaviours with high probability of detection under a variety of scenarios.

The remainder of the paper is organized as follows. In Section II, the framework of the MEC-enabled spectrum blockchain is introduced, and the three-stage consensus of the MEC-enabled spectrum blockchain is designed in details. In Section III, the numerical simulation results are provided to evaluate the security performance in defending Byzantine attack of spectrum data falsification. Conclusions and future works are provided in Section IV.

2 A Mobile Edge Computing Enabled Spectrum Blockchain

Existing work [6] considers SMDs and SUDs should be networked in a cloud-based architecture to achieve efficient spectrum data sharing and exchanging. However, as the growing of spectrum data, the cloud-based architecture becomes impractical. The reasons are analyzed as follows.

Spectrum data can be regarded as an important type of big data. If we use 1 byte to represent the spectrum data in a geospatial grid of 100 m $\times$100 m, a frequency resolution of 100 kHz, and a time resolution of 100 ms, after one week, for a frequency band ranging from 0 to 5 GHz and a geospatial area of 100 km $\times$100 km, the total spectrum data size will reach [6]:

$$\begin{aligned}&\frac{7\,\text{days}}{\text{week}}\times\frac{24\,\text{hours}}{\text{day}}\times\frac{3600\,\text{seconds}}{\text{hour}}\times\frac{1\,\text{seconds}}{100\,\text{ms}}\\&\quad\times\frac{5\,\text{GHz}}{100\,\text{kHz}}\times\frac{100\,\text{km}\times100\,\text{km}}{100\,\text{m}\times100\,\text{m}}\times1\,\text{Byte}\\&=3.024\times10^{17}\ \text{Byte/ week}\\&=3.024\times10^{5}\ \text{Terabyte}\left(\text{TB}\right)\text{/week}\end{aligned}\tag{1}$$

By comparison, Facebook, one of well-known big data example, generates approximately 3.5 $\times 10^3$TB per week. The amount of spectrum data is more than 80 times that of Facebook in the same duration. Furthermore, the volume of spectrum data grows with the time duration, frequency range, and spatial scale, as well as the corresponding resolution in each dimension. Whether uploading spectrum data to the cloud or downloading it locally will generate massive communication traffic and cause unbearable latency. However, spectrum data is regarded as a special big data, majority spectrum data is generally collected and consumed locally and consumed locally. It is unnecessary and costly to store entire spectrum data centrally in the spectrum server cloud. It is considered that relying only on the cloud-based architecture is inadequate to realize efficient spectrum data storing and high-quality spectrum inference for IoSD.

The proposed mobile edge computing enabled spectrum blockchain is illustrated in Figure. 1. Spectrum data serve as transactions and are packaged to generate spectrum blocks, which are

linked in chronological order to form spectrum blockchain. The spectrum block contents include the arbitrary nonce, the hash of the previous spectrum block, and the root hash of listed spectrum data, which is linked in Merkle tree structure [10]. However, the blockchain suffers from various disadvantages, particularly in terms of quickly reaching consensus in a vast network, energy consumption in computation, and the storage requirements of the entire chain for verification.

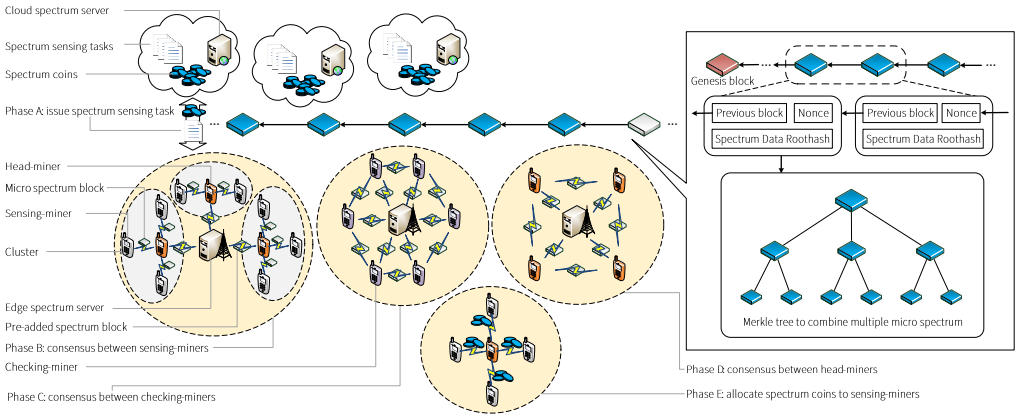


Fig. 1. Framework of MEC-enabled spectrum blockchain.

It should be noted that the SMDs and SUDs are generally deployed at the edge of IoSD, and the features of spectrum data mentioned above. MEC is employed to address the flaws of blockchain, which was firstly proposed by the European Telecommunications Standard Institute (ETSI) in 2014, and was defined as a new platform that ”provide IT and cloud-computing capabilities within the Radio Access Network (RAN) in close proximity to mobile subscribers” [11]. Compared to the cloud-based architecture, MEC has the advantages of achieving lower latency, saving sensing energy for personal mobile devices, supporting context-aware spectrum inference, and enhancing privacy preserving.

Traditionally, a miner is required to solve a compute-intensive PoW and obtain a hash value so as to append a new block to the current blockchain. After solving the PoW, the pre-added block and the hash value are broadcast to the other miners in the network for validation. The new block is successfully added if majority of miners reach consensus. The consensus mechanism gives a reward to the successful miner as an incentive. A cryptocurrency usually serves as the reward, such as Bitcoin [12]. However, it should be noted that PoW is probabilistic in nature: miners strive to find a special value (usually less than a target value) to achieve the blocks hash, thus in the PoW-based consensus mechanism, a smaller hash value still likely to be obtained after the previous block is verified and added to the blockchain.

Basically, there are two kinds consensus mechanism: PoW and PBFT. PoW is operated on th basis of purely computation protocols that use proof of computation to randomly select a node which single-handedly decides the next operation. PBFT is purely communication based protocols in which nodes have equal votes and go through multiple rounds of communication to reach consensus. Therefore, PoW suffers from non-finality, that is a block appended to a blockchain is not confirmed until it is verified by majority of miners. For example, eclipse attacks on Bitcoin [13] exploit this probabilistic guarantee to allow double spending. While PBFT is finality, once a block is appended, it is final and cannot be replaced or modified. The scalability is the key problem for PBFT, as it incurs $O(N^2)$ network messages for each round of

agreement where N is the number of nodes in the network [14]. In practice, the PBFT protocol scales poorly and even collapse before reaching consensus.

Instead of PoW, based on the PBFT protocol, a three-stage mechanism is designed to achieve consensus at the edge of IoSD, which realize the efficient and non-probabilistic block appending for spectrum blockchain. The basic operation cycle is combined by five phases, which is shown Figure. 1. The procedure of consensus achievement mainly involves Phase B, Phase C, and Phase D, i.e. the consensus between sensing-miners, checking miners, and head-miners. In the following, we first elaborate the basic operation cycle of the MEC enabled spectrum blockchain, then provide the detailed consensus mechanism.

2.1 MEC Enabled Spectrum Blockchain

The basic operation cycle of the MEC enabled spectrum blockchain can be generally divided into five phases, which are briefly illustrated in Figure. 1.

Phase A: a spectrum server issues a spectrum sensing task and deposits some spectrum-coins on IoSD. The spectrum sensing task specifies the requirements, including the sensing duration, frequency range and geographic area. All SMDs and SUDs on the IoSD can query for the list of spectrum sensing task in executing, and determine to participate one of them. Spectrum-coin is a cryptocurrency that generates and circulates in IoSD, which can be used to purchase the spectrum data and the spectrum access opportunities.

Phase B: the SMDs within the required geographic area determine to participate the spectrum sensing task and form several clusters spontaneously. One SMD becomes the head-miner of the cluster and the other SMDs become the sensing-miners. The sensing-miners perform spectrum sensing to collect spectrum data under the leadership of the head-miner, then sensing-miners and head-miner of the cluster perform the consensus mechanism in distributional manner to achieve the common value about the spectrum data. Afterwards, each miner of the cluster obtain identical values of spectrum data. The head-miner of each cluster encrypt the spectrum data with private key and upload it to the edge base station to form the pre-added spectrum block. Each user in IoSD keeps a pair of keys, i.e. public key and private key. The public key exposes in IoSD and is used for encryption, while the private key is kept in individuals and is used for decryption [17].

Phase C: the head-miner uploads the pre-added spectrum block and deposits some spectrum-coins to IoSD as the checking rewards. Then, some personal wireless devices other than the sensing-miners in Phase B, which deployed at the same edge of IoSD, register and become checking-miners. These checking-miners download and decrypt the pre-added spectrum block with their private key. The consensus mechanism is performed between checking-miners to determine whether the pre-added spectrum block satisfies the requirement.

Phase D: the last stage consensus is performed between the head-miners that their blocks have pass the checking in previous phase. The errors are calculated between these uploaded blocks and pre-added blocks, the block with the smallest error with the pre-added spectrum block is determined as the optimal spectrum block, and the head-miner have the right to append their block to the spectrum blockchain.

Phase E: once the head-miner have appended the block to the spectrum blockchain, the spectrum-coin deposited in the IoSD is released to the cluster, and allocated automatically according to their contribution to the appended spectrum block, e. g. the structure of Merkle tree. Then, the spectrum sensing task is completed, the spectrum sensing data is recorded in the structure of Merkle tree and stored at the edge of IoSD. SUDs deployed in the geographical area can download the spectrum data from the edge base station at the expense of some spectrum-

coin, then infer the spectrum access strategy and purchase spectrum access opportunities. The consensus between head-miners encourages personal wireless devices to make efforts improve the sensing performance, so as the pre-added spectrum blocks can be appended to the spectrum blockchain, and obtain the spectrum-coin finally. Lets image an extreme case that no spectrum block pass the checking, indicates that the spectrum sensing task is failed, then the spectrum-coin is released back to the spectrum server.

2.2 Three-stage Consensus Mechanism

In this paper, a three-stage mechanism, i.e. the consensus between sensing-miners, checking miners, and head-miners, is designed to reach consensus in appending block to the spectrum blockchain. The three-stage mechanism mainly involves Phase B, Phase C, and Phase D, the briefly procedure of which is illustrated in Figure. 1.

Specifically, the consensus between sensing-miners in Phase B is designed to determine the optimal value of spectrum data, which can be regard as a Byzantine failure tolerance mechanism in case of attack by malicious users, such as spectrum data falsification and faking state value during iteration; the consensus between checking-miners in Phase C is served as a distribution-based Byzantine defense mechanism, which perform a quickly verification to determine whether a Byzantine attack occurs in Phase B, in order to make the decision on accept the pre-added block or not; the consensus between head-miners in Phase D is designed to determine which cluster has the right to append the block to the blockchain and obtain the reward. The full consensus procedure is elaborated as follows.

The first stage is the consensus between sensing-miners that occurs in Phase B. Let miner_{ij}^{S} denotes the j-th sensing-miner of cluster C_i, i=1,2,...,N and j=1,2,...,k_i, where there are N clusters in the IoSD and k_i sensing-miners in cluster C_i. miner_{ij}^{S} first collects the spectrum data through spectrum sensing. Afterwards, miner_{ij}^{S} exchanges the spectrum data Data_{ij} with his edge neighbours at time k=0, i.e. $x_{ij}(0)=\mathrm{Data}_{ij}$. Then, miner_{ij}^{S} performs local calculation to get updated states $x_{ij}(k+1)$ at time k=1,2,.... The iterations are repeatedly done until all the states of the cluster $x_{ij}(k)$ converge to a common value x^*. For simplicity, we assume all the sensing-miners perform energy detection and obtain the measurement Y_{ij} at time k=0, i.e. $x_{ij}(0)=Y_{ij}$. From time k=1,2,..., miner_{ij}^{S} begins to exchange the measurements Y_i, i=1,2,...,k_i with his edge neighbours. The iteration of the consensus mechanism is denoted as follows [15]:

$$x_{ij}(k+1)=x_{ij}(k)+\eta\sum_{n\in\mathcal{N}_j}\left(x_{in}(k)-x_{ij}(k)\right) \tag{2}$$

where

$$0<\eta\le\left(\max_j\left|\mathcal{N}_j\right|\right)^{-1}\triangleq\frac{1}{\Omega}, \tag{3}$$

where $\mathcal{N}_j$ is denoted as the neighbors of miner_{ij}^{S}, and $|\mathcal{N}_j|$ is the degree of miner_{ij}^{S}. Ω is the maximum degree of the adjacency matrix $\boldsymbol{G}$ [16]. The iteration of the consensus-based algorithm can also be written in vector form

$$\boldsymbol{x}(k+1)=\boldsymbol{P}\boldsymbol{x}(k), \tag{4}$$

where $\boldsymbol{P}=\boldsymbol{I}-\eta\boldsymbol{L}$, and $\boldsymbol{I}$ is identity matrix, $\boldsymbol{L}$ is the Laplacian transform of $\boldsymbol{G}$. The iterations are repeatedly performed until the measurement $x_{ij}(k+1)$ converge to an identical value x^*. The convergence of the consensus-based algorithm is considered as follows.

Theorem 1: Consider a cluster of sensing-miners

$$x_{ij}(k+1) = x_{ij}(k) + u_{ij}(k), \tag{5}$$

with the adjacency matrix $\boldsymbol{G}$ applying the consensus-based algorithm (8), where $u_{ij} = \eta \sum_{n \in \mathcal{N}_j} \left(x_{in}(k) - x_{ij}(k) \right)$, $0 < \eta \le 1/\Omega$. Then, two propositions can be derived:

(1) A consensus is asymptotically achieved for all initial states;

(2) An identical value of the consensus-based algorithm can be asymptotically achieved with the limit $x^* = \frac{1}{n} \sum_{i=1}^{n} x_i(0)$ for all the individual measurements.

According to Theorem 1, if η satisfies $0 < \eta \le 1/\Omega$, then the consensus can be achieved, and the identical value $x^* = \frac{1}{n} \sum_{i=1}^{n} x_i(0)$ is the average of the initial vector $\boldsymbol{x}(0)$. The derivation of the common value x^* denotes the accomplishment of the consensus between sensing-miners.

The second stage is the consensus between checking-miners that occurs in Phase C. The SMDs or SUDs first download the pre-added spectrum block from edge base station and decrypt it with their private keys. When decrypt the pre-added spectrum block, the checking-miners obtain the list of spectrum data, which contain the locations of the spectrum sensing, the adjacency matrix of the cluster, and the values for some frequency range. Then, the checking-miners deployed at same edge of IoSD perform consensus to check whether the spectrum data is falsified by the malicious users or experience some collapse in Phase B. When the consensus is completed between checking-miners, an common value $x_i^{\dagger}$ is derived and the confidence interval $[\Delta_{\min}, \Delta_{\max}]$ is calculated under confidence level $1-\alpha$. If $x_i^{\dagger}$ falls into $[\Delta_{\min}, \Delta_{\max}]$, it is considered there is no malicious user between sensing-miners and the pre-added spectrum block is accepted, otherwise the checking-miner consider there are some malicious users between sensing-miners and the pre-added spectrum block is rejected.

The third stage is the consensus between head-miners that occurs in Phase D, with the aim of appending new block to spectrum blockchain and determining which cluster provide the new spectrum block. These head-miner of each cluster first starts the consensus procedure and exchanges the spectrum data with its neighboring head-miners. The consensus value of spectrum data Q^* is derived and the cluster has the smallest difference with Q^* wins the spectrum-coin and its spectrum block is appended to the spectrum block. It should be noted that through the PBFT-based consensus mechanism, the new appended block is deterministic and permanent. While the MEC has greatly reduced the communication overhead.

3 Simulation Results And Discussions

The simulations are mainly performed at the edge of IoSD, which is assumed to be a 5000 m × 5000 m rectangle region. All personal wireless devices are deployed in the region, including the sensing-miners, the checking-miners, and the edge base station. For the emulational simplicity, a primary transmitter is assumed to be deployed at regional center, SMDs and SUDs are randomly distributed in the region. One deployment scenario of 6 clusters is shown in Fig. 2, which contains 10 sensing-miners for each cluster.

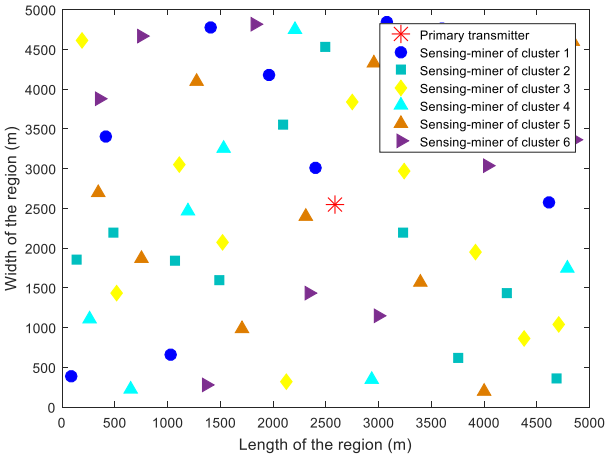
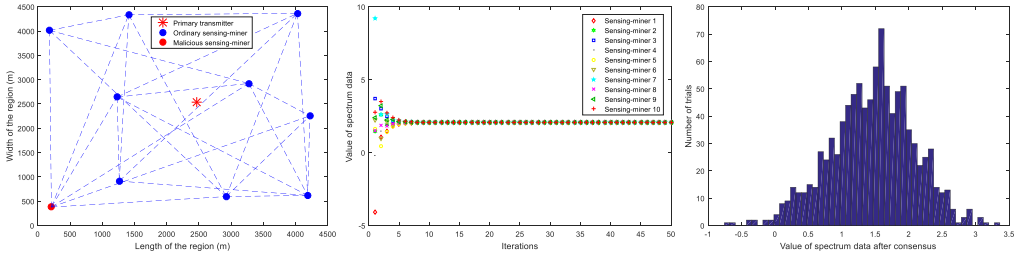


Fig. 2. Deployment of personal wireless devices in IoSD.

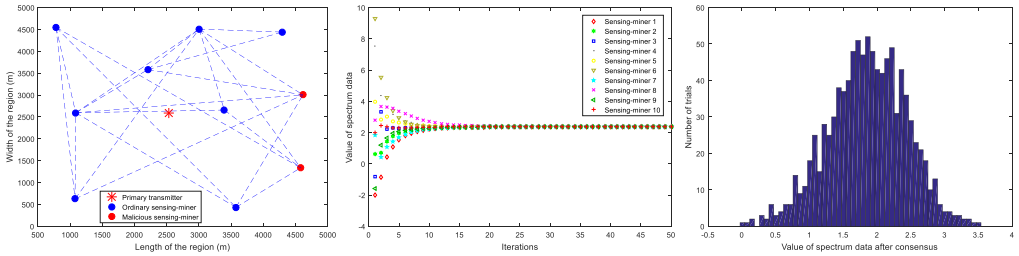
The sensing-miners first perform local spectrum sensing to collect spectrum data. The signal of primary transmitter is assumed to experiences Rayleigh fading. If the primary transmitter keeps silence, the measurement Y_{ij} only contains additive Gaussian white noise, which follows a chi-square distribution of 0 dB average SNR. If the primary transmitter is active, the measurement Y_{ij} is the sum of two independent random variables [18]. Each sensing-miner receives different average SNR varying from 5 dB to 15 dB, which is related to the location, distance, and propagation path.

Afterwards, each sensing-miner exchanges spectrum data with his neighbors. As shown in Fig. 3(a), (d), and (g), the communication links are illustrated by blue dash lines, which are generated randomly and represented by adjacency matrix $\boldsymbol{G}$. Each sensing-miner updates sensing data when receiving information from neighbors, i.e. compares the value of spectrum data and discards the value with maximum deviation, and also exclude the corresponding neighbor. This process is performed iteratively until convergence. Fig. 3(b), (e), and (h) show the procedure of consensus, it is assumed there are 1∼3 malicious users in the cluster (less than1/3 of total users that specified by PBFT as the of fault tolerance), and these malicious users send a sensing value that is opposite to his observation. It can be observed from consensus procedures that the consensus can be reach under Byzantine attack (1∼3 malicious users), and the consensus value falls outside the confidence interval. To clearly illustrate the performance in defending malicious users, we have performed 20000 Monte-Carlo trails and summarized the checking results in Table. 1. It can be seen that the proposed consensus mechanism can basically defend all Byzantine attacks. The defending performance decreases sightly with the increasing of malicious users.

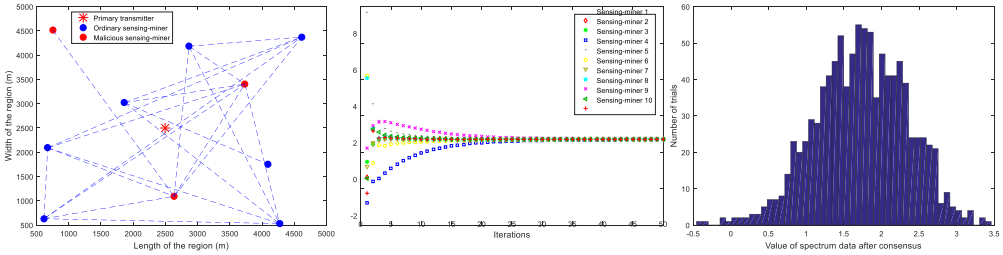
At last, the consensus in head-miners with the aim of determine which cluster provide the optimal spectrum block. It is assumed there are 6 pre-added spectrum blocks pass the checking, corresponding to 6 clusters. Fig. 4(b) shows the procedure of consensus mechanism under the network topology of Fig. 4(a). A consensus value Q^*=3.0184 is derived and the 4th block with the smallest difference, i.e. The block of the 4th cluster is appended to the spectrum blockchain, and the corresponding spectrum-coin is allocated automatically in the 4th cluster according the contribution of sensing-miners to the Merkle tree.



(a) Deployment of cluster **(b)** Consensus procedure **(c)** Distribution of spectrum data value



(d) Deployment of cluster **(e)** Consensus procedure **(f)** Distribution of spectrum data value

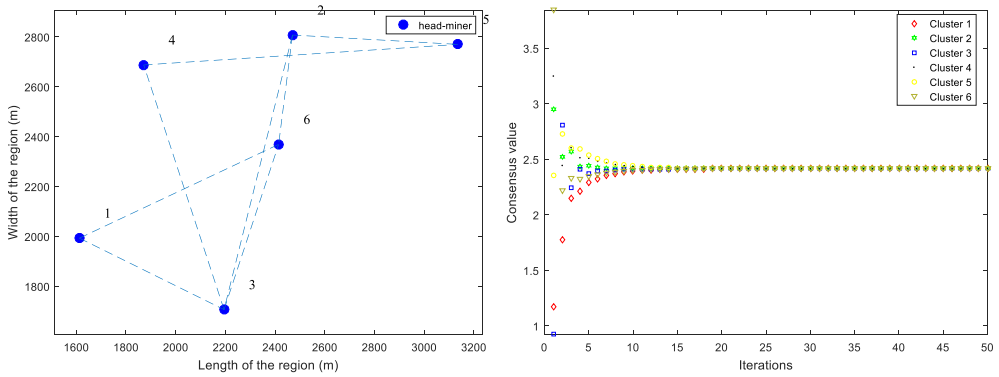


(g) Deployment of cluster **(h)** Consensus procedure **(i)** Distribution of spectrum data value

Fig. 3 Consensus procedure of MEC-enabled spectrum blockchain

Table 1. Checking Results of Monte-Carlo Trails

Number of malicious users	Confidence interval	Probability of detection
1	[-0.8896,0.9292]	99.8%
2	[-0.8180,0.8930]	97.6%
3	[-0.7842,0.8561]	95.5%



(a) Deployment of head-miners **(b)** Consensus procedure

Fig. 4 Consensus procedure of MEC-enabled spectrum blockchain

4 Conclusion

We have developed a MEC-enabled spectrum blockchain for IoSD, which applies a three-stage consensus mechanism to achieve secure and immutable spectrum data monitoring and sharing, and employs the edge-deployed personal wireless device to realize efficient storage of massive spectrum data and quickly response of spectrum strategy customization. The benefit of the MEC-enabled spectrum blockchain can be summarized in two-folds: (i) the security and immutability of spectrum blockchain inspire personal wireless devices to monitor and share spectrum data; (ii) the MEC-enabled spectrum data sharing will greatly empowered an accurate and reliable customization of spectrum access strategy. Further investigation include: (i) the security performance the proposed PBFT-based consensus mechanism is still need to be evaluated through various Byzantine attack modes; (ii) the energy efficiency and processing latency of the proposed MEC-enable spectrum blockchain are still need to be measured.

References

[1] J. Mitola, J. Guerci, J. Reed, Y. Yao, Y. Chen, et al.. Accelerating 5G QoE via public-private spectrum sharing. IEEE Communications Magazine, vol. 52, no. 5, pp. 77-85, (2014)

[2] G. Ding, J. Wang, Q. Wu, Y. Yao, F. Song and T. A. Tsiftsis. Cellular-base-station-assisted device-to-device communications in TV white space. IEEE Journal on Selected Areas in Communications, vol. 34, no. 1, pp. 107-121, (2016)

[3] M. Höyhtyä, Aarne Mämmelä, X. Chen, A. Hulkkonen, J. Janhunen. Database-assisted spectrum sharing in satellite communications: a survey. IEEE Access, vol. 5, pp. 25322-25341 (2017)

[4] G. Ding, F. Wu, Q. Wu, S. Tang, F. Song, et al.. Robust online spectrum prediction with incomplete and corrupted historical observations. IEEE Transactions on Vehicular Technology, vol. 66, no. 9, pp. 8022-8036 (2017)

[5] R. Etkin, A. Parekh, and D. Tse. Spectrum sharing for unlicensed bands. IEEE Journal on Selected Areas in Communications, vol. 25, no. 3, pp. 517-528 (2007)

[6] Q. Wu, G. Ding, Z. Du, Y. Sun, M. Jo, and A. V. Vasilakos. A cloud-based architecture for the internet of spectrum devices over future wireless networks. IEEE Access, vol. 4, pp. 2854-2862, 2016.

[7] K. Kotobi and S. G. Bilen. Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access. IEEE Vehicular Technology Magazine, vol. 13, no. 1, pp. 32-39 (2018)

[8] Y. Mao, C. You, J. Zhang, K. Huang and K. B. Letaief. A survey on mobile edge computing: the communication perspective. IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322-2358 (2017)

[9] M. Chiang and T. Zhang. Fog and IoT: an overview of research opportunities. IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854-864 (2016)

[10] R. Merkle. Secrecy, authentication, and public key systems. Ph. D. Dissertation, Stanford University (1979)

[11] Mobile-edge computing-Introductory technical white paper. White Paper, ETSI, Sophia Antipolis, France (2014). [Online].
Available: https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf

[12] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system. (2008)

[13] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. in Proc. of 24th USENIX Security Symposium (USENIX Security), Washington, D.C., USA, pp. 129-144 (2015)

[14] T. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, et al. Untangling Blockchain: a data processing view of Blockchain systems. IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385 (2018)

[15] Z. Li, F. R. Yu, and M. Huang, A distributed consensus-based cooperative spectrum-sensing scheme in cognitive radios. IEEE Transactions on Vehicular Technology, vol. 59, no. 1, pp. 383-393 (2010)

[16] M. Huang and J. H. Manton. Coordination and consensus of networked agents with noisy measurements: Stochastic algorithms and asymptotic behavior. SIAM Journal on Control and Optimization, vol. 48, no. 1, pp. 134-161 (2009)

[17] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A first look at the usability of bitcoin key management. in Proc. of Workshop on Usable Security (2015)

[18] F. Digham, M.-S. Alouini, and M. Simon. On the energy detection of unknown signals over fading channels. in Proc. IEEE ICC, Anchorage, AK, vol. 5, pp. 3575-3579 (2003)